Wireless Glossary

#

100BaseT — A synonym for the Fast Ethernet networking standard. The *100* refers to a maximum data-transfer rate of 100 megabits per second over twisted-pair wiring.

10BaseT — A synonym for the Ethernet networking standard. The *10* refers to a maximum data-transfer rate of 10 megabits per second over twisted-pair wiring.

3DES — Three-DES (data encryption standard). As its name suggests, 3DES is a three-step data encryption algorithm that evolved from DES.

802.11 — A set of IEEE standards for data transmission over wireless LANs. The specs include 802.11, 802.11a, 802.11b, and 802.11g. All of the specifications use the Ethernet protocol.

- **802.11** describes a wireless LAN that operates in the 2.4GHz range and provides a data transmission rate of 1Mbps or 2Mbps using spread spectrum technology.
- **802.11a** describes a wireless LAN that operates in the 5GHz frequency range and provides a data transmission speed of up to 54Mbps.
- **802.11b** is the most widespread wireless LAN standard. It describes a wireless LAN that operates in the 2.4GHz frequency range with a data transmission speed of up to 11Mbps using spread spectrum technology. (This specification was also known as Wi-Fi, but that term now encompasses newer standards such as 802.11a and 802.11g.)
- **802.11g** describes a wireless LAN that operates in the 2.4GHz frequency range. It provides a data transmission speed (over short distances) of up to 54Mbps using orthogonal frequency division multiplexing (OFDM) technology.

802.1x is a security standard for wired and wireless LANs.

A

access point — Wirelessly networked devices usually connect to a wired LAN through a hardware device called an access point. Multiple access points, set up in various locations around an office, let users roam from office to conference room to coworker's cubicle while staying connected.

ad-hoc mode — Also known as peer-to-peer mode or IBSS, ad-hoc mode lets wirelessly networked devices communicate directly, without going through an access point or other intermediary.

adapter — An adapter comes in many forms, but it's essentially a device that connects to or installs into your computer, adding a specific capability or feature.

AES — Advanced Encryption Standard. The Advanced Encryption Standard is a data encryption scheme that trumps DES and even 3DES by using three different key sizes (128-bit, 192-bit, and 256-bit) but only one encryption step to encrypt data in 128-bit blocks.

antenna gain — This describes an antenna's transmission power as a ratio of its output (send) signal strength to its input (receive) signal strength. It is usually expressed in dBi; a higher dBi means a stronger antenna.

AP — See access point.

ADSL — Asymmetric Digital Subscriber Line. ADSL uses standard phone lines to provide high-speed data communications. ADSL providers typically deliver upstream (from the user) speeds that top out at 128Kbps and downstream (to the user) speeds of no more than 1.5Mbps. A separate phone line is not required to obtain ADSL service.

B

bandwidth — This term describes data-carrying ca-

pacity — in other words, how much (and how fast) data flows on a given transmission path. Bandwidth is commonly measured in bits or bytes per second.

beacon — In wireless networking, a beacon is a packet sent by a connected device to inform other devices of its presence and readiness.

beacon interval — When a wirelessly networked device sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again.

Bluetooth — Bluetooth is a wireless computing and telecommunications specification that defines how mobile personal computing devices work with each other and with regular computer and phone systems within a close range.

BSS — Basic Service Set. When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID — The unique identifier for an access point in a BSS network. See SSID for more details.

C

cable — A broadband transmission technology using coaxial cable or fiber-optic lines.

CDMA — Code Division Multiple Access. CDMA is a technique used mainly with personal communications devices such as mobile phones that digitizes the conversation and tags it with a special frequency code. The data is then scattered across the frequency band in a pseudorandom pattern. The receiving device is instructed to decipher only the data corresponding to a particular code to reconstruct the signal.

Cat-5 — Category 5 cabling is used in Ethernet and Fast Ethernet networks.

client — The customer side of a client/server setup. When you log on to a server, the word *client* can refer to you, to your computer, or to the software running on your computer.

coaxial cable — Typically used to connect a television to cable TV services, coaxial cable consists of a small copper tube or wire surrounded by an insulating material and another conductor with a larger diameter, usually in the form of a tube or a copper braid. This cable is then encased in a rubberized protective material.

D

decibel/dB — A mathematical (specifically, logarithmic) ratio that indicates the relative strength of a device's electric or acoustic signal to that of another.

dBi — Decibels compared to an isotropic antenna. The higher the dBi, the stronger the antenna.

dBm — Decibels compared to one milliwatt. The higher the dBm, the greater the device's transmit or receive power.

DES — Data Encryption Standard. DES is an encryption method that uses an algorithm for private-key encryption, in which the sender uses the same private key to send the message that the recipient uses to decode it.

DHCP — Domain Host Control Protocol. DHCP is a protocol for dynamically assigning IP addresses to networked computers.

dipole antenna — A type of antenna commonly used with wireless networking devices. It has a signal range of 360 degrees horizontally and 75 degrees vertically. It works best in offices, away from exterior walls where signals could leak out.

directional antenna — This term defines several types of antennae that redirect the signal received from a transmitter to enhance its strength in a certain direction, unlike an omnidirectional antenna.

DMZ — Demilitarized Zone. Networking has coopted the term, originally used to define a closely monitored no-man's land placed between rival nations, and used it to refer to an unprotected subnet connected to a local network but outside the peripheries of a firewall. A DMZ allows you to protect certain computers behind a firewall while allowing one or more other computers full exposure to other networks. A DMZ is often used for servers or gaming computers that require full access to the Internet in order to function properly.

DNS — Domain Name System. The DNS is the international network of Internet domain name servers, names, and addresses that enables you to locate other computers on the Internet.

DSL — Digital Subscriber Line. Digital subscriber lines carry data at high speeds over standard telephone wires.

DSSS — Direct Sequence Spread Spectrum. DSSS is a spread spectrum radio technology. The sender alters, or modulates, the signal by spreading it over a wider frequency, generating what seems like signal noise to everyone except the receiver who knows how to return the signal to its original form, or demodulate it.

DTIM — Delivery Traffic Indication Message. A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

DTIM interval — A DTIM interval, also known as a Data Beacon Rate, is the frequency at which an access point's beacon will include a DTIM. This frequency is usually measured in milliseconds (ms) or its equivalent, kilomicroseconds (Kmsec).

dual-band radio — A radio device is dual-band if it can send and receive signals from two frequencies—in the case of wireless networking, both the 2.4GHz and 5GHz bands.

dynamic DNS — The DNS would quickly run out of IP addresses if every Web-browsing computer user in the world were assigned a permanent one. Dynamic DNS is the system by which ISPs or companies are assigned a pool of IP addresses that they can assign to any user only for the time needed, so the same IP addresses can be used repeatedly for different people in different sessions.

E

EAP — Extensible Authentication Protocol. When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). LCP is somewhat inflexible, however, because it has to specify an authentication device early in the process. EAP lets the system gather more information from the user before deciding which authenticator to use; it's called extensible because it allows more authenticator types than LCP did, such as passwords, public keys, or biometrics.

EAP-MD5 — Extensible Authentication Protocol-Message Digest 5. EAP-MD5 is an EAP security algorithm developed by RSA Security that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication.

EAP-TLS — This high-security version of EAP requires authentication from both the client and the server. If one of them fails to offer the appropriate authenticator, the connection is terminated.

encryption — Encryption is the process of changing data into a form that can be read only by the intended receiver.

ESS — Extended Service Set. ESS is the collective term for two or more BSSs that use the same switch in a LAN.

ESSID — Extended Service Set Identifier. An ESSID is the unique identifier for an ESS. See SSID for more details.

Ethernet — Ethernet is a standard for connecting computers into a local-area network (LAN). Ethernet is also called 10BaseT, which denotes a peak transmission speed of 10Mbps using copper twisted-pair cable.

F

Fast Ethernet — Also known as 100BaseT, Fast Ethernet is an upgraded standard for connecting computers in a local-area network (LAN). Fast Ethernet works just as regular Ethernet (also known as 10BaseT) does, except that it can transfer data at a peak rate of 100Mbps. It's also more expensive and less common than its slower 10BaseT sibling.

FCC — Federal Communications Commission. The government agency responsible for regulating telecommunications in the United States.

FHSS — Frequency Hopping Spread Spectrum. A type of spread spectrum radio technology where the sender and receiver "hop" together from one frequency to another to avoid detection or jamming.

firewall — A system that prevents unauthorized users from logging in to a private network (usually one that's connected to the public Internet). It can also be used to keep users inside the firewall from accessing computers outside the firewall. A firewall could be a dedicated computer equipped with security measures such as a dial-back feature, a software-based protection, or a combination of both. The firewall screens incoming server requests to make sure they come from authorized sources. For instance, a company might authorize outside users from certain IP addresses to access its intranet.

fragment — In networking, a packet whose size exceeds the bandwidth of the network is broken into smaller pieces called fragments.

fragmentation length — In a network, the maximum size or length of a fragment is determined by the protocol used to transport the data.

FTP — File Transfer Protocol. This Internet protocol is used to copy files between computers — usually a client and an archive site.

G

gateway — A combination of a software program and piece of hardware that passes data between networks. Though most likely you're not aware of it, you typically encounter a gateway when you log

on to an Internet site or when you send e-mail to someone who uses a different e-mail system than you do. In wireless networking, gateways can also serve as security and authentication devices, access points, and more.

H

HomePlug — A home-networking standard where devices connect using cables plugged into regular AC outlets, removing the need for running physical cables or configuring a wireless network.

hot spot — In wireless networking, a hot spot is a specific part of an access point's range in which the general public can walk up and use the network. The service may be available only for a fee, and the hot spot's range is usually short to control the physical proximity of the user. In some parts of the world, it is called a cool spot.

hub — This piece of networking hardware serves as a central connection point for multiple PCs or other devices (usually on a wired or wireless Ethernet network). A passive hub simply transmits data from any of its connected devices to the rest of the network. An active or manageable hub can also monitor network traffic and configure its ports.

I

IBSS — Independent Basic Service Set. See ad-hoc mode.

ICS — See Internet connection sharing.

IEEE — Institute of Electrical and Electronics Engineers. Pronounced "eye-triple-E," this nonprofit U.S. engineering organization develops, promotes, and reviews standards within the electronics and computer science industries.

infrastructure mode — When a wireless network functions in infrastructure mode, every user communicates with the network and other users through an access point; this is the typical way corporate WLANs work. An alternative is ad-hoc mode, but users would have to switch to infrastructure mode to access a network's printers and servers.

Internet connection sharing — Also known as ICS, this is a Windows XP function that lets home or small-office users with networked computers share one Internet connection. A computer with an Internet connection serves as the ICS host for all the computers.

intranet — A play on the word *Internet*, an intranet is a restricted-access network that works like the web but isn't on it. Usually owned and managed by a corporation, an intranet enables a company to share its resources with its employees without confidential information being made available to everyone with Internet access.

IP address — Internet Protocol address. This address is a 32-bit, unique string of numbers that identifies a computer, a printer, or another device on the Internet. The IP address consists of a quartet of numbers separated by periods.

ISM band — The 2.4GHz frequency spectrum is also known as the ISM band. *ISM* is not actually synonymous with 2.4GHz, however; it stands for Industrial, Scientific and Medical, the noncommercial uses for which the 2.4GHz band and other frequencies were once reserved by the ITU-T.

isotropic antenna — A theoretical, ideal antenna whose signal range is 360 degrees in all directions. It is used as a baseline for measuring a real antenna's signal strength, in dBi, where the *i* stands for *isotropic antenna*.

ITU-T — International Telecommunications Union-Telecommunication. The newer name for the international committee CCITT, ITU-T has a long way to go until it's as well known as its older counterpart.

L

LAN — Local-Area Network. A local-area network is a short-distance network used to link a group of computers together, usually within a building. Ethernet is the most commonly used type of LAN.

M

MAC address — Media Access Control address. Each device connected to an Ethernet network has a unique numeric identifier called a MAC address, which is used for data transmission and security functions.

MAC filtering — MAC filtering is like using a guest list to restrict entry to a party. A network checks a device's MAC address against a database to see if it's authorized to access the network.

Mbps — Megabits per second. A megabit is roughly a million bits of data. This abbreviation is used to describe data transmission speeds, such as the rate at which information travels over the Internet.

modem — An external box or internal circuitry that converts computer data into sound that can be transmitted over phone lines. First used to send telegrams, early modems alternated between two different tones. This is called *modulation*, and the

process of modulating (and demodulating at the receiving end) gave the modem its name.

N

NAT — Network Address Translation. NAT solves both security and efficiency issues surrounding Internet use by letting a network at, say, a company, use its own pool of IP addresses for internal communications and another pool of addresses for external communications. This method hides internal IP addresses from hackers. In addition, because NAT lets the same IP addresses be used internally by multiple companies, it reduces the demand for globally unique, static IP addresses.

NIC — Network Interface Card. An adapter inside a computer that lets the computer connect to a network via a wired or wireless transmission medium.

O

OFDM — Orthogonal Frequency Division Multiplexing. A wireless transmission technique that splits a signal into smaller signals that are then transmitted at different frequencies simultaneously.

omnidirectional antenna — This is like a dipole antenna because it radiates its signal 360 degrees horizontally; however, its signal is flatter than a dipole's, allowing for higher gain.

P

packet — While it may seem as though you send or receive a continuous stream of data every time you use the Internet, you don't. Instead, it's more efficient to break up the transmission into pieces called packets. These packets contain information about which computer sent the data and where the data is going.

PAN — Personal-Area Network. A PAN is distinct from a LAN because it's a casual, close-proximity network where connections are made on the fly and temporarily. Meeting attendees, for example, can connect their Bluetooth-enabled notebook computers to share data across a conference room table, but they break the connection once the meeting is over. See also WPAN.

PC Card — A credit card-size peripheral that plugs into a special slot on portable computers (and some desktop models). The card may add RAM, a modem or network adapters, a hard drive, or another device. These PC Cards conform to several standards set by the PCMCIA and were originally called PCMCIA Cards.The original Type I PC Card is 3.3mm thick, a format used mainly to add RAM. Type II cards are thicker (5mm) and often are used for modems and NICs (though they're also used for RAM). Type III cards are much thicker (10.5mm) and often are used for hard disks and radio devices. A PC Card slot on a computer is usually designated by the thickest card it can accommodate. A Type II PC Card slot, for instance, can take a Type I PC Card as well as a Type II (and it might be called a Type I/II), but it cannot fit a Type III.

PCI — Peripheral Component Interconnect. If you have a Pentium system, it's extremely likely that it runs a self-configuring PC local bus called PCI.

PCMCIA — Personal Computer Memory Card International Association. This stands for the name of a trade association founded in 1989 to establish standards for expansion cards for portable computers. Based in Sunnyvale, California, the PCMCIA's specifications for the PC Card enabled the computer industry to manufacture credit-card-size removable cards to add RAM, modems, network adapters, hard disks, and even radio devices such as pagers and global positioning systems to portable computers.

ping — When submarine crews wanted to determine the distance of an object from themselves, they'd send a sonar ping and wait to hear the echo. In the computer world, Ping is a program that "bounces" a request (in other words, sends a packet) over the Internet to another computer to see if the remote computer is still responding. If the ping comes back, the remote computer is still connected.

port — In networking, a server's various functions, such as managing FTP traffic or maintaining the DNS list, are each assigned a virtual address called a port. Any requests for that function are sent to the port address.

port forwarding — This lets a computer external to a secured network access a computer on the network through the mapping of a port on the network's firewall to a port on a specified computer.

PPP — Point-to-Point Protocol. PPP is the Internet standard for serial communications. Newer and better than its predecessor, SLIP, PPP defines how your modem connection exchanges data packets with other systems on the Internet.

PPTP — Point-to-Point Tunneling Protocol. PPTP is a protocol developed by a number of compa-

nies, including Microsoft, that allows secure transmission of data in TCP/IP packets. PPTP and similar protocols are used to carry secure communications over Virtual Private Networks that use public phone lines.

protocol — Because so many different types of computers and operating systems connect via modems or other connections, they have to follow communications standards called protocols. The Internet is a heterogeneous collection of networked computers and is full of different protocols, including PPP, TCP/IP, SLIP, and FTP.

proxy server — A system that caches items from other servers to speed up access. On the web, a proxy first attempts to find data locally, and if it's not there, fetches it from the remote server where the data resides permanently.

Q

QoS — Quality of Service. QoS can be used to describe any number of ways in which a network provider guarantees a service's performance, such as an average or minimum throughput rate.

R

RADIUS — Remote Authentication Dial-In User Service. The RADIUS is a server database used by an ISP to authenticate users who are trying to log on to the service. It can also track network usage.

RAM — Random Access Memory. When you run an application such as Microsoft Word, the program is called up from its permanent storage area (like the hard drive, floppy disk, or CD-ROM) and moved into the RAM, where it sends requests to the CPU. Using faster memory means your information spends less time in line before being processed. Your computer should have as much RAM as possible so that it can work efficiently.

RJ-11 — Registered Jack 11. This is the standard telephone connector — a tab snaps into the socket and has to be pressed to remove the connector from the wall or your phone. An ordinary phone circuit uses two wires. The RJ-11 jack has room for up to four wires, but at a glance it's easy to mistake it for the larger RJ-45 jack, which can house up to eight wires.

RJ-45 — Registered Jack 45. RJ-45 connectors look a bit like standard phone connectors (RJ-11) but are twice as wide (with eight wires). RJ-45s are used for hooking up computers to LANs or for phones with lots of lines.

router — As the name indicates, this piece of hardware routes data from one local-area network to another or to a phone line's long-distance line.

RTS — Request To Send. An RTS is a message sent by a networked device to its access point, seeking permission to send a data packet. See also RTS threshold.

RTS threshold — Request To Send threshold. The RTS threshold specifies the packet size of an RTS transmission. This helps control traffic flow through an access point, especially one with many clients.

S

server — The business end of a client/server setup, a server is usually a computer that provides the information, files, web pages, and other services to the client that logs on to it. (The word *server* is also used to describe the software and operating system designed to run server hardware.)

SLIP — A standard for connecting to the Internet with a modem over a phone line. It has serious trouble with noisy dial-up lines and other error-prone connections, so look to higher-level protocols such as PPP for error correction.

spread spectrum — A wireless communications technology that scatters data transmissions across the available frequency band in a pseudorandom pattern. Spreading the data across the frequency spectrum greatly increases the bandwidth (amount of data that can be transmitted at one time), and it also makes the signal resistant to noise, interference, and snooping.

SSID — Service Set Identifier. Every wireless network or network subset (such as a BSS, ESS, or IBSS) has a unique identifier called an SSID (and may be called a BSSID, ESSID, and so on, depending on what it is identifying).

SSL — Secure Sockets Layer. SSL is an Internet protocol that uses public-key and secret-key encryption to secure data sent from one server to another.

static IP address — See IP address.

switch — A device in a network that selects the path that a data packet will take to its next destination. The switch opens and closes the electrical circuit to determine whether — and where — data will flow. On the Internet, the switch sits at the point that connects one network to another network.

T

TCP/IP — Transmission Control Protocol/Internet Protocol. TCP/IP is the method by which data is

sent across the Internet. These two protocols were developed by the U.S. military to allow computers to talk to each other over long-distance networks.

throughput — A general term used when defining how much data is going how quickly over a particular transport medium, such as a wireless network or a phone line. When your modem says it can transfer data at a rate of 56Kbps, for instance, it's describing its maximum throughput level.

twisted pair — Telephone companies commonly run twisted pairs of copper wires to each customer household. The pairs consist of two insulated copper wires twisted into a spiral pattern. Although originally designed for plain old telephone service (POTS), these wires can carry data as well as voice. New services such as ISDN and ADSL also use twisted-pair copper connections.

U

UPnP — Universal Plug and Play. Universal Plug and Play is a networking architecture developed by a consortium of companies to ensure easy connectivity between products from different vendors. UPnP devices should be able to connect to a network automatically, handling identification and other processes on the fly. The standards developed by the UPnP Forum are media-, platform-, and device-independent.

UWB — Ultra Wide Band. An emerging wireless technology that sends signals in extremely short pulses over a wide swath of the radio frequency spectrum.

V

virtual server — The part of a server that functions as if it were a separate, dedicated server. Each virtual server can run its own operating system and applications and even be networked with other virtual servers on the same machine. Web hosting companies use virtual servers to house multiple clients' web sites on one server, for instance.

VPN — Virtual Private Network. A private network of computers that's at least partially connected by public phone lines. A good example would be a private office LAN that allows users to log in remotely over the Internet (an open, public system).

W

WAN — Wide-Area Network. Take two local-area networks (LANs), hook them together, and you have a WAN. Wide-area networks can be made up of interconnected smaller networks spread throughout a building, a state, or the entire globe. The Internet could be considered a WAN. A wireless WAN is called a WLAN.

warchalking — The unauthorized act of physically marking the locations of wireless access points (APs) that are available for free network access, such as those at a coffee house or an airport — or an office AP with a leaky signal. The word *chalking* derives from the informal system of markings used by vagabonds to indicate places where one might get a meal or a place to sleep. See also wardriving.

wardriving — The unauthorized act of seeking out and mapping wireless access points (APs) that are available for free network access, such as those at a coffee house or an airport — or an office AP with a leaky signal. This is the new, wireless version of war dialing, in which hackers dialed hundreds of numbers to find an open modem so that they could gain access to a company's network. See also warchalking.

WECA — Wireless Ethernet Compatibility Alliance. This is the former name of the Wi-Fi Alliance of vendors promoting 802.11 wireless networking standards and compatibility.

WEP — Wired Equivalent Privacy. All 802.11b (Wi-Fi) networks use WEP as their basic security protocol. WEP secures data transmissions using 64-bit or 128-bit encryption; however, it does not offer complete security and is usually used in conjunction with other security measures such as EAP.

Wi-Fi — Wireless Fidelity. Wi-Fi originally referred to the 802.11b specification for wireless LANs, but it is now used to describe any of the 802.11 wireless networking specifications.

wireless bridging — A networking bridge is used to connect two or more separate networks. A wireless bridge functions the same way but can be used in situations in which running a wire or cable would be impractical or prohibitively expensive, such as creating a 10-mile point-to-point link.

wireless channel — Different networking technologies divide their allocated spectrum up in different ways. You can sometimes improve the performance of your network and avoid interference on the band by moving your network to a different nonoverlapping channel available to the devices. 802.11b and 802.11g devices have three nonoverlapping channels. 802.11a devices have eight nonoverlapping channels.

WLAN — Wireless Local-Area Network. A wirelessly

connected LAN, such as an 802.11 network.

WPA — Wi-Fi protected access. WPA is a specification for improving the security of Wi-Fi networks, replacing the weaker WEP for current and future 802.11 standards. It uses 802.1x and EAP to restrict network access, and it uses its own encryption, called Temporal Key Integrity Protocol (TKIP), to secure data during transmission.

WPAN — Wireless Personal-Area Network. A WPAN is specifically a PAN that uses wireless connections, but because all current PAN technologies, such as Bluetooth, are wireless, you can consider the terms synonymous.

X

Xmodem — A protocol for transferring files during direct dial-up communications. Developed by Ward Christensen in 1977, Xmodem does basic error checking to ensure that information isn't lost or corrupted during transfer; it sends data in 128-byte blocks. Xmodem has undergone a couple of enhancements: Xmodem CRC uses a more reliable error-correction scheme, and Xmodem-1K transfers data faster by sending it in 1,024-byte blocks.